DISCIPLINE: Confidentiality and Integrity

Discipline Roadmap for: SIEM (Security Information & Event Management)

DOMAIN: SECURITY

Current	2 Years	5 Years
Baseline Environment	**Tactical Deployment**	**Strategic Direction**
OSSIM (Open source Security Info. Mgt.) →	→	Market Watch
Cisco MARS →	→	
Computer Associates →	→	
IBM →	→	
Novell →	→	
netForensics →	→	

Shared	Agency
✓	✓

Retirement Targets

N/A

Mainstream Platforms (must be supported)

OSSIM, Cisco MARS, Computer Associates, IBM, Novell, netForensics

Containment Targets

N/A

Emerging Platforms

Market Watch - OSSIM

Implications and Dependencies

- Costs and implementation considerations can be substantial (~$30,000 - $150,000).

Roadmap Notes

- OSSIM – Low cost, fully functional Open source product for medium (1,000 units) and small enterprises.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

DISCIPLINE: Confidentiality and Integrity

Discipline Roadmap for: SIEM (Security Information & Event Management)

- **Discipline Boundaries:**
  - SIEM technology is composed of two basic capabilities: Security Information Management (SIM) and Security Event Management (SEM). SIM provides data analysis and reporting of historical events, often used to support regulatory requirements. SEM provides real-time data collection and correlation, often used to support incident response capabilities.
- **Discipline Standards:**
  - Currently, there are no SIEM specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - The South Carolina Information and Analysis Center (SC-ISAC) is an education and awareness initiative, jointly developed by the SC Joint Terrorism Task Force (JTTF), the State's Chief Information Office (CIO), the Federal Bureau of Investigation (FBI), and the US Secret Service (USSS). SC-ISAC's mission is to protect the State's citizenry and economy by safeguarding its critical information infrastructure. To that end, SC-ISAC offers a number of security services, including incident response and reporting. Therefore, State Agencies should contact SC-ISAC to develop an integrated incident response plan. Detailed information concerning SC-ISAC can be found on the WWW at http://secure.sc.gov, or by contacting the CIO's Director of Security Policy and Assessment at (803) 896-1660.
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007